REMARKS

The Examiner is thanked for the performance of a thorough search. By this amendment, claims 3, 16, 29 and 39 are canceled. Claims 24-26, 33-36 and 39 were previously canceled. Hence, claims 1-2, 4-15, 17-23, 27-28, 30-32, 37-38 and 40-50 are pending in this application. The amendments to the claims do not add any new matter to this application. Furthermore, the amendments to the claims were made to improve the readability and clarity of the claims and not for any reason related to patentability. All issues raised in the Office Action mailed March 25, 2008 are addressed hereinafter.

I. ISSUES NOT RELATING TO PRIOR ART

A. CLAIM OBJECTIONS

CLAIMS 7, 20, 43 AND 47

Claims 7, 20, 43 and 47 are rejected under 35 U.S.C. § 1.75(c) as being of improper dependent form for failing to further limit the subject matter of a previous claim.

Applicants believe that the objection is fully addressed by amended claims 7, 20, 43 and 47.

Reconsideration and withdrawal of the objection is respectfully requested.

II. ISSUES RELATING TO PRIOR ART

A. CLAIMS -- 35 U.S.C. § 103: BUER, BEN

Claims 1-3, 5-7, 11, 14-16, 18-20, 24, 27-29, 31-32, 37-39, 41-43 and 47 are rejected under 35 U.S.C. § 103(a) as being allegedly anticipated by Buer et al. (U.S. Patent Application Publication No. 2004/0005061), hereafter "Buer," and in view of Benayoun et al. (U.S. Patent No. 6,804,257), hereafter "Ben." (Office Action, page 3) The rejection is respectfully traversed.

CLAIM 1

Present claim 1 recites:

1. A method for applying a quality of service to an encrypted packet comprising:

during initial establishment of a secure control channel, receiving and storing an identifier associated with the quality of service in association with a first Internet Key Exchange (IKE) ID;

examining an encrypted packet;

without decrypting the encrypted packet, mapping a second IKE ID from the packet, using the first IKE ID, to the identifier associated with the quality of service in a profile portion of the encrypted packet;

in response to mapping to the identifier associated with the quality of service, applying the associated quality of service to the encrypted packet.

The Office Action acknowledges that "Buer does not disclose [...] receiving and storing an identifier associated with the quality of service [...]," but relies upon Ben (column 6, lines 1-33) to show "**during initial establishment of a secure control channel, receiving and storing an identifier associated with the quality of service in association with a first Internet Key Exchange (IKE) ID.**" (Office Action, pages 3-4) This is incorrect.

Ben describes an initialization sequence in a communication network. Ben's initialization sequence can have starting headers, which are sent in the clear, i.e., not encrypted. (Ben: column 5, lines 62-65) Examples of starting headers may include headers carrying out labels for conventional quality of service (QoS) functions. (Ben: column 6, lines 3-8)

However, conventional QoS functions are unrelated to Internet Protocol Security (IPsec), including the Internet Key Exchange (IKE) protocol, which is one of the IPsec implementations. While QoS functions handle data flow performance issues, IKE functions handle security issues in the Internet Protocol communications. While QoS manages data flow priorities, IKE manages authentication and encryption of data packets. Ben's conventional quality of service labels are not **associated with any IKE identifiers,** as claimed.

Further, a combination of the references provides no suggestion to map an IKE identifier to QoS value in the manner claimed. In fact, Ben lacks the concept of having **"QoS identifiers** associated with **IKE** identifiers." Nowhere in the specification does Ben talk about IKE, IKE

identifiers, or other aspects of IPsec. Ben's starting headers do not comprise IKE identifiers, and Ben does not describe any association between IKE identifiers and QoS identifiers.

In sharp contrast to Ben, claim 1 recites that "**during initial establishment of a secure control channel, […] an identifier which is associated with the quality of service, is received and stored in association with a first Internet Key Exchange (IKE) ID**." As described in applicants' specification (paragraphs 40-41 and 60), using the IKE identifiers to identify QoS treatments has a number of benefits. For example, instead of sending the same QoS and IKE data in each data packet for each user within a class of users, storing associations between QoS identifiers and IKE identifiers for classes of users allows equal application of the same QoS to each user within the class. Further, indexing a set of IKE functions and QoS functions, using just one identifier sent in the clear in the packet, allows execution of QoS on the packet before a time-consuming decryption of the packet even begins.

Storing associations between QoS identifiers and IKE identifiers during an initial establishment of the secure control channel is also beneficial in VPN environments, as described in applicants' specification (paragraph 60). For example, in a VPN environment, where customers use overlapping address spaces within the internal networks, IPsec would cause encrypting of the payload of an original packet, and thus obscure the original packet header containing QoS instructions. Obscuring the original packet header makes the QoS instructions unreadable, and thus, makes it impossible to apply QoS in accordance with the original packets contents until the packet is actually decrypted. However, if, "**during initial establishment of a secure control channel, […] an identifier associated with the quality of service in association with a first Internet Key Exchange (IKE) ID is received and stored,**" as in claim 1, the association between the IKE identifiers and the QoS identifiers is created, and can be used to retrieve the QoS identifiers indirectly using a mapping approach. This provides an efficient service mechanism, wherein QoS functions can be identified using just IKE identifiers. Subsequently, QoS functions can be successfully applied to IPsec protected (encrypted) packets.

(Specification, paragraph 60) This is not taught or suggested in Buer and Ben individually or in combination.

Further, Buer and Ben fail to describe "**without decrypting the encrypted packet, mapping a second IKE ID from the packet, using the first IKE ID, to the identifier associated with the quality of service in a profile portion of the encrypted packet**," as claimed.

The Office Action concedes that Buer reads an identifier from a packet merely to determine what security association is involved – not to determine what QoS to apply. Any "service" descried in Buer merely involves conventional decryption based on a particular security association. Further, Buer has no description of "**mapping a [...] IKE ID from the packet to the identifier associated with the quality service in a profile portion of the encrypted packet,"** because Buer's identifiers are not used to map the IKE identifiers' space to the QoS identifiers' space.

Further, before Buer can apply any QoS, Buer has to decrypt the packet because Buer's QoS function is carried in the encrypted portion of the packet. Therefore, in Buer, the only "**identifiers associated with the QoS,"** are QoS identifiers that require decrypting before they can be understood.

Ben deals with **"identifiers associated with the quality of service**," not with IKE identifiers. In particular, Ben does not **"map a second IKE ID from the packet, using the first IKE ID, to the identifier associated with the quality of service,"** as claimed. As discussed above, Ben carries QoS identifiers in starting headers, which are sent in the clear, i.e. not encrypted. However, Ben's QoS identifiers are independent from IKE identifiers. Since Ben does not store "**an identifier [...] associated with the quality of service, [...] in association with a first Internet Key Exchange (IKE) ID**," Ben cannot **"map [...] IKE ID to the identifier associated with the quality of service,"** as claimed.

Further, Ben cannot access IKE identifiers without decrypting an encrypted packet. In Ben, only synchronization headers and starting headers are sent in the clear, but neither one

carries IKE identifiers. Therefore, to even check whether an IKE identifier is carried in Ben's packet, Ben has to decrypt the packet first.

In sharp contrast to Buer and Ben, claim 1 recites that "**without decrypting the encrypted packet,** by **mapping a second IKE ID from the packet, using the first IKE ID, […] the identifier associated with the quality of service in a profile portion of the encrypted packet** is retrieved. Claim 1 requires that **"without decrypting the encrypted packet, […] a second IKE ID"** is retrieved and used to retrieve the QoS **identifier** from the association stored "**during initial establishment of a secure control channel."** This feature is not described in Buer and Ben.

Finally, Buer and Ben fail to describe "**in response to mapping to the identifier associated with the quality of service, applying the associated quality of service to the encrypted packet."**

Since Buer and Ben, individually and in combination, fail to describe the **"mapping a second IKE ID from the packet, using the first IKE ID, to the identifier associated with the quality of service in a profile portion of the encrypted packet,"** Buer and Ben fail to describe **"apply[ing] the associated quality of service to the encrypted packet in response to** that **mapping."**

Therefore, at least one element of claim 1 is not disclosed, taught or suggested by the combined prior art. Thus, it is respectfully submitted that Buer and Ben, individually and in combination, fail to disclose the complete subject matter recited in claim 1.

Reconsideration and withdrawal of the rejection is respectfully requested.

CLAIMS 14, 27 AND 37

Claims 14, 27 and 37 recite features similar to those in claim 1. Therefore, applicants believe that claims 14, 27 and 27 are patentable over Buer and Ben for the same reasons discussed for claim 1.

B. CLAIMS -- 35 U.S.C. § 103(a): BUER, BEN AND PIPER

Claims 4, 8, 17, 21, 30, 40, 44 and 48 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Buer and Ben and in view of Piper's "The Internet IP Security Domain of Interpretation for ISAKMP" (November, 1998). (Office Action, page 7) The rejection is respectfully traversed.

Claims 4 and 8 depend directly or indirectly from claim 1, claims 17 and 21 depend directly or indirectly from claims 14, claim 30 depends indirectly from claim 27, and claims 40, 44 and 48 depend directly or indirectly from claim 37. As discussed above, Buer and Ben, individually and in combination, fail to teach and suggest independent claims 1, 14, 27 and 37.

Further, Piper fails to cure the deficiencies of Buer and Ben with respect to independent claims 1, 14, 27 and 37. Therefore, because Buer, Ben and Piper, individually and in combination, fail to provide all subject matter recited in claims 1, 8, 14, 27 and 37, and due to claim dependency, claims 4, 8, 17, 21, 30, 40, 44 and 48 are patentable over Buer in view of Ben and in further view of Piper.

Reconsideration and withdrawal of the rejection are respectfully requested.

C. CLAIMS -- 35 U.S.C. § 103(a): BUER, BEN AND VALENCI

Claims 9-10, 12, 22-23, 45-46 and 49-50 are rejected under 35 U.S.C. § 103(a) as being allegedly anticipated by Buer and Ben and in view of Valenci et al. (U.S. Patent Publication No. 2003/0005279), hereafter "Valenci." (Office Action, page 9) The rejection is respectfully traversed.

Claims 9-10 and 12 depend directly or indirectly from claim 1, claims 22-23 depend directly or indirectly from claim 14, and claims 45-46 and 49-50 depend directly or indirectly from claim 37. As discussed above, Buer and Ben, individually and in combination, fail to teach and suggest independent claims 1, 14, 27 and 37.

Further, Valenci fails to cure the deficiencies of Buer and Ben with respect to independent claims 1, 14, 27 and 37. Therefore, because Buer, Ben and Valenci, individually and in combination, fail to provide all subject matter recited in claims 1, 14, 27 and 37, and due

to claim dependency, claims 9-10, 12, 22-23, 45-46 and 49-50 are patentable over Buer in view of Ben and in further view of Valenci.

Reconsideration and withdrawal of the rejection are respectfully requested.

D. CLAIM 13

Claim 13 is rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Buer and Ben and in view of Ylonen et al. (U.S. Patent Publication No. 2002/0062344), hereafter "Ylonen." (Office Action, page 10) The rejection is respectfully traversed.

Claim 13 depends indirectly from claim 1. As discussed above, Buer and Ben, individually and in combination, fail to teach and suggest independent claim 1. Further, Ylonen fails to cure the deficiencies of Buer and Ben with respect to independent claim 1. Therefore, because Buer, Ben and Piper, individually and in combination, fail to provide all the subject matter recited in claim 1, and due to claim dependency, claim 13 is patentable over Buer in view of Ben and in further view of Ylonen.

Reconsideration and withdrawal of the rejection are respectfully requested.

E. DEPENDENT CLAIMS

The claims that are not discussed above depend directly or indirectly on the claims that have been discussed. Therefore, those claims are patentable for the reasons given above. In addition, each of the dependent claims separately introduces features that independently render the claim patentable. However, due to the fundamental differences already identified, and to expedite positive resolution of the examination, separate arguments are not provided for each of the dependent claims at this time.

III. CONCLUSION

For the reasons set forth above, all of the pending claims are in condition for allowance. A petition for an extension of time is hereby made to the extent necessary to make this reply

timely filed. If any applicable fee is missing or insufficient, the Commissioner is authorized to charge any applicable fee to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: June 04, 2008

/MalgorzataAKulczycka#50496/
Malgorzata A. Kulczycka
Reg. No. 50, 496

2055 Gateway Place, Suite 550
San Jose, California 95110-1089
Telephone No.: (408) 414-1228
Facsimile No.: (408) 414-1076